SECURITY ANALYSIS REPORT

HTTP Security Headers Assessment

Target URL:
https://ine.com

Scan Date:
August 15, 2025 at 12:42 AM UTC

Overall Security Score:
65/100

Risk Level:
■ **Medium**

Prepared by:
CyberHeaders Security

CONFIDENTIAL

This report contains sensitive security information and should be treated as confidential.
Distribution should be limited to authorized personnel only.

Table of Contents

1. Executive Summary

Assessment Overview

Our comprehensive security analysis has evaluated the HTTP security headers implementation for **https://ine.com**. This automated assessment identified critical security gaps that require immediate attention to protect against common web vulnerabilities.

Key Findings:

- Overall Security Score: **65/100**
- Risk Classification: ■ **Medium**
- Total Security Recommendations: **14**
- High-Priority Actions: **5**

Business Impact

The identified vulnerabilities expose your organization to potential security breaches, including cross-site scripting (XSS), clickjacking, and man-in-the-middle attacks. Immediate implementation of our recommendations will significantly strengthen your security posture and protect sensitive user data.

Next Steps

We recommend prioritizing the high-risk findings detailed in Section 3 and implementing the security recommendations in order of priority. Our team is available to assist with remediation efforts and ongoing security monitoring.

2. Priority Findings Quick Reference

The following table summarizes the highest priority security findings that require immediate attention:

Priority	Finding	Severity	Action Require
#1	Add missing security header: x-content-type-options	HIGH	Immediate
#2	Add missing security header: x-xss-protection	HIGH	Immediate
#3	Add missing security header: referrer-policy	HIGH	Immediate
#4	Add missing security header: permissions-policy	MEDIUM	Soon
#5	Add missing security header: cross-origin-opener-policy	MEDIUM	Soon

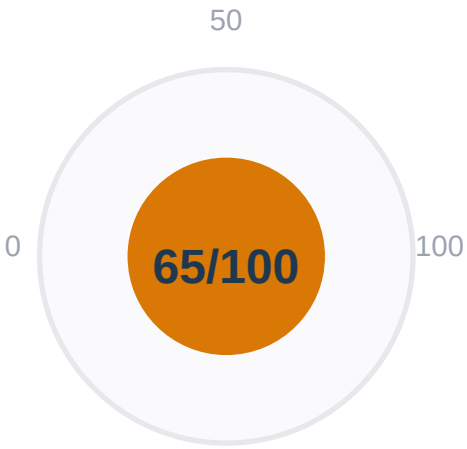
3. Scan Overview & Metrics

5.1 Scan Details

Property	Value
Target URL	https://ine.com
Scan Date	August 15, 2025 at 12:42 AM UTC
Security Score	65/100
Risk Level	■ Medium

Total Findings	14

5.2 Security Score Visualization

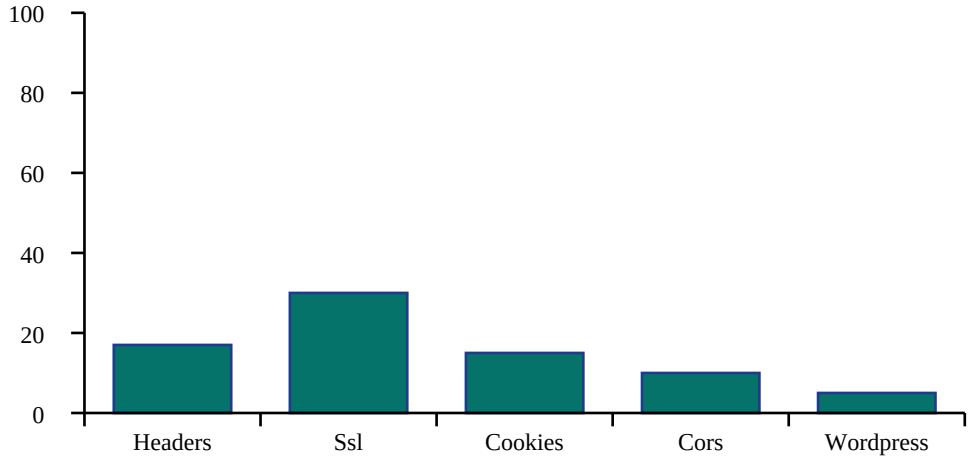


5.3 Security Category Analysis

The following analysis shows performance across different security categories:

Security Category	Score	Rating	Status
Headers	17/100	Poor	✗
Ssl	30/100	Poor	✗
Cookies	15/100	Poor	✗
Cors	10/100	Poor	✗
Wordpress	5/100	Poor	✗

Security Category Scores



4. Detailed Security Findings

6.1 Critical Missing Security Headers

The following essential security headers are missing and must be implemented immediately:

- **x-content-type-options** - Critical security header not implemented

Impact: Missing x-content-type-options exposes users to security vulnerabilities

Recommendation: Implement x-content-type-options with appropriate security policies

- **x-xss-protection** - Critical security header not implemented

Impact: Missing x-xss-protection exposes users to security vulnerabilities

Recommendation: Implement x-xss-protection with appropriate security policies

- **referrer-policy** - Critical security header not implemented

Impact: Missing referrer-policy exposes users to security vulnerabilities

Recommendation: Implement referrer-policy with appropriate security policies

• **permissions-policy** - Critical security header not implemented

Impact: Missing permissions-policy exposes users to security vulnerabilities

Recommendation: Implement permissions-policy with appropriate security policies

• **cross-origin-opener-policy** - Critical security header not implemented

Impact: Missing cross-origin-opener-policy exposes users to security vulnerabilities

Recommendation: Implement cross-origin-opener-policy with appropriate security policies

• **cross-origin-embedder-policy** - Critical security header not implemented

Impact: Missing cross-origin-embedder-policy exposes users to security vulnerabilities

Recommendation: Implement cross-origin-embedder-policy with appropriate security policies

• **cross-origin-resource-policy** - Critical security header not implemented

Impact: Missing cross-origin-resource-policy exposes users to security vulnerabilities

Recommendation: Implement cross-origin-resource-policy with appropriate security policies

6.2 Deprecated Security Headers

The following deprecated headers should be removed to prevent information disclosure:

• **server** - Deprecated header revealing server information

Impact: Information disclosure may aid attackers in reconnaissance

Recommendation: Remove or replace server with modern alternatives

6.3 Content Security Policy Vulnerabilities

Critical Content Security Policy configuration issues:

• CSP missing important directive: default-src

Impact: CSP misconfigurations can lead to XSS vulnerabilities

• CSP missing important directive: script-src

Impact: CSP misconfigurations can lead to XSS vulnerabilities

• CSP missing important directive: object-src

Secur

Impact: CSP misconfigurations can lead to XSS vulnerabilities

• CSP missing important directive: base-uri

Impact: CSP misconfigurations can lead to XSS vulnerabilities

5. Security Recommendations

The following recommendations are prioritized by security impact. Address high-priority items first:

1. ■ HIGH Add missing security header: x-content-type-options
2. ■ HIGH Add missing security header: x-xss-protection
3. ■ HIGH Add missing security header: referrer-policy
4. ■ HIGH Add missing security header: permissions-policy
5. ■ HIGH Add missing security header: cross-origin-opener-policy
6. ■ MEDIUM Add missing security header: cross-origin-embedder-policy
7. ■ MEDIUM Add missing security header: cross-origin-resource-policy
8. ■ MEDIUM Remove deprecated header: server
9. ■ MEDIUM CSP issue: CSP missing important directive: default-src
10. ■ MEDIUM CSP issue: CSP missing important directive: script-src
11. ■ LOW CSP issue: CSP missing important directive: object-src
12. ■ LOW CSP issue: CSP missing important directive: base-uri
13. ■ LOW CORS issue: Overly permissive CORS policy: Access-Control-Allow-Origin: *
14. ■ LOW HSTS issue: HSTS missing includeSubDomains directive

6. Expert AI Security Analysis

Security Assessment of https://ine.com

• *1. Executive Summary:**

The security scan of https://ine.com reveals a medium-risk security posture (score 65/100). The primary vulnerabilities stem from missing and improperly configured security headers, specifically concerning Content Security Policy (CSP) and several crucial HTTP headers designed to mitigate XSS, clickjacking, and other attacks. While SSL/TLS configuration appears sound, the lack of comprehensive header protection significantly weakens the website's overall security. Addressing the identified vulnerabilities is crucial to reduce the risk of exploitation.

• *2. Critical Vulnerabilities:**

• **Missing Critical Security Headers:** The absence of several crucial security headers (x-content-type-options, x-xss-protection, referrer-policy, permissions-policy, cross-origin-opener-policy, cross-origin-embedder-policy, cross-origin-resource-policy) represents a major vulnerability. These headers are essential for preventing various attack vectors, including MIME-sniffing, XSS, and information leakage.

• **Insufficient Content Security Policy (CSP):** The CSP is incomplete, missing directives for `default-src`, `script-src`, `object-src`, and `base-uri`. This leaves the website vulnerable to various attacks, including script injection and data manipulation.

• **Overly Permissive CORS Policy:** The `Access-Control-Allow-Origin: *` indicates an overly permissive CORS policy, potentially allowing unauthorized access to resources from any origin. This needs immediate attention.

• *3. Security Header Analysis:**

• **Present and Properly Configured:** `content-security-policy`, `x-frame-options`, `strict-transport-security` (although missing `includeSubDomains`). The presence of `Strict-Transport-Security` (HSTS) is positive, ensuring HTTPS usage, but the omission of `includeSubDomains` limits its effectiveness.

• **Missing Headers:** A significant number of crucial security headers are missing, as detailed in the key findings. This is a critical weakness.

• **Deprecated Header:** The presence of the `server` header should be removed as it reveals server information, potentially aiding attackers.

• *4. WordPress-Specific Risks (if applicable):**

The report indicates no WordPress-specific issues. However, the identified vulnerabilities could still impact a WordPress site, especially if plugins or themes are not properly secured.

• *5. SSL/TLS Configuration Review:**

The SSL/TLS configuration appears satisfactory. No weak cipher suites are used, and TLS compression is disabled, mitigating known vulnerabilities.

• *6. Actionable Recommendations:**

• **Implement Missing Security Headers:** Immediately add all missing headers (x-content-type-options, x-xss-protection, referrer-policy, permissions-policy, cross-origin-opener-policy, cross-origin-embedder-policy, cross-origin-resource-policy) with appropriate values.
• **Complete the Content Security Policy (CSP):** Implement a comprehensive CSP, defining explicit sources for scripts, styles, images, and other resources. Avoid using `unsafe-inline`, `unsafe-eval`, and overly broad directives like `*`.
• **Restrict CORS Policy:** Replace `Access-Control-Allow-Origin: *` with a specific list of allowed origins. Only allow access from trusted domains.
• **Improve HSTS:** Modify the `Strict-Transport-Security` header to include the `includeSubDomains` directive.
• **Remove Deprecated Header:** Remove the `server` header to prevent information disclosure.
• **Regular Security Scanning:** Implement regular automated security scans to proactively identify and address vulnerabilities.
• **Vulnerability Management:** Establish a process for addressing identified vulnerabilities promptly and effectively.
• **Security Awareness Training:** Educate website developers and administrators on secure coding practices and common web vulnerabilities.

• *7. Overall Risk Assessment:**

The website's current security posture is **medium risk**. While the SSL/TLS configuration is strong, the numerous missing and misconfigured security headers significantly increase the risk of exploitation. The lack of a comprehensive CSP and overly permissive CORS policy are particularly concerning. Implementing the recommendations above is crucial to mitigate these risks and improve the website's overall security score to an acceptable level. A reassessment should be conducted after implementing the recommended changes.

7. Methodology & Disclaimer

Assessment Methodology

This security assessment was conducted using automated scanning techniques that analyze HTTP response headers for security configurations. Our analysis includes:

• Evaluation of essential security headers (HSTS, CSP, X-Frame-Options, etc.)
• Detection of deprecated or information-leaking headers
• Content Security Policy validation and vulnerability assessment
• SSL/TLS configuration analysis
• Cookie security evaluation

• CORS policy review

Limitations & Disclaimer

This automated assessment provides a comprehensive overview of HTTP security header implementation but does not constitute a complete security audit. For thorough security assurance, we recommend:

• Manual penetration testing
• Code review and vulnerability assessment
• Infrastructure security evaluation
• Social engineering assessments

Important Notice: This report is confidential and intended solely for the organization that requested the assessment. The findings and recommendations should be implemented by qualified security professionals.

Thank You

Thank you for choosing **CyberHeaders Security** for your security assessment needs. We are committed to helping organizations strengthen their security posture through comprehensive analysis and actionable recommendations.

This automated assessment provides valuable insights into your HTTP security headers configuration. For a more comprehensive security evaluation, we recommend conducting additional penetration testing and manual security reviews.

Contact Information

Contact Type	Details
Technical Support	Email: security@cyberheaders.com Phone: +1 (555) 123-4567
Business Inquiries	Email: sales@cyberheaders.com Phone: +1 (555) 765-4321
Website	https://www.cyberheaders.com
Address	CyberHeaders Security 123 Security Boulevard Cyber City, CC 12345 United States

Follow-up Services Available

- **Detailed penetration testing** - Comprehensive security assessment
- **Security architecture review** - Infrastructure and design analysis
- **Compliance assessments** - Regulatory compliance verification
- **Security training and awareness** - Staff education programs
- **Incident response planning** - Emergency response preparation

Contact us to discuss how we can further enhance your security posture.